

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-054488

(43)Date of publication of application : 19.02.2004

(51)Int.Cl.

G06F 13/00

H04L 12/66

(21)Application number : 2002-209576

(71)Applicant : YOKOGAWA ELECTRIC CORP

(22)Date of filing : 18.07.2002

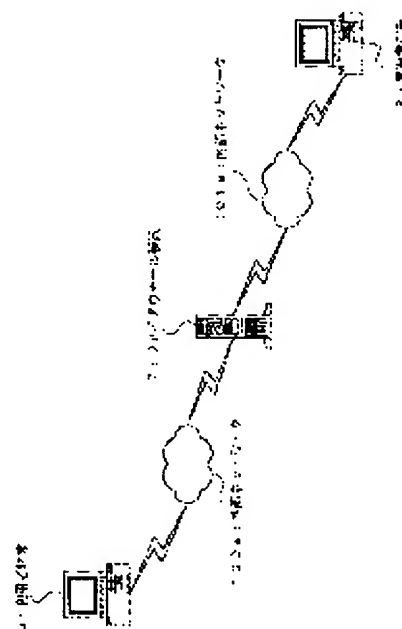
(72)Inventor : ARAI TAKAYUKI

## (54) FIREWALL DEVICE

## (57)Abstract:

PROBLEM TO BE SOLVED: To realize a firewall device capable of temporarily changing access limit without generating erroneous setting or security deterioration.

SOLUTION: This firewall device for limiting any illegal access to an internal network is provided with a firewall means connected to an external network for limiting any illegal access to the internal network, a setting interface means connected through the firewall means to an external network for fetching the changed contents of the setting of the firewall means, and a setting changing means for authenticating whether or not a user is preliminarily registered and authorized to use through the setting interface means, and for limiting the setting items settable for each authenticated user, and for changing the setting of the firewall means after evaluating the legality of the changed contents.



(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2004-54488

(P2004-54488A)

(43) 公開日 平成16年2月19日(2004. 2. 19)

(51) Int. Cl.<sup>7</sup>

G06F 13/00

H04L 12/66

F I

G06F 13/00

H04L 12/66

3 5 1 Z

B

テーマコード (参考)

5B089

5K030

審査請求 未請求 請求項の数 10 O L (全 13 頁)

(21) 出願番号 特願2002-209576 (P2002-209576)

(22) 出願日 平成14年7月18日 (2002. 7. 18)

(71) 出願人 000006507

横河電機株式会社

東京都武蔵野市中町2丁目9番32号

(72) 発明者 新井 貴之

東京都武蔵野市中町2丁目9番32号 横

河電機株式会社内

Fターム(参考) 5B089 GA04 GA11 JA32 KA17 KB13

KC14 KC52 KC58

5K030 GA15 HC01 HC13 HD03 HD06

(54) 【発明の名称】 ファイアウォール装置

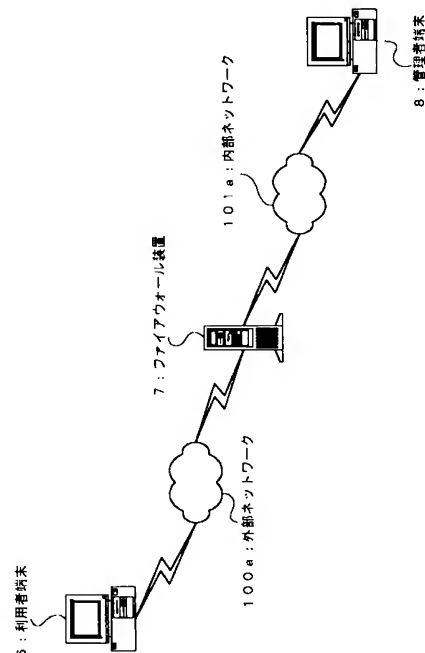
(57) 【要約】

【課題】 誤設定やセキュリティの低下を招くことなくアクセス制限の一时的な変更が可能なファイアウォール装置を実現する。

【解決手段】 内部ネットワークへの不正なアクセスを制限するファイアウォール装置において、内部ネットワークに対する不正なアクセスを制限する外部ネットワークに接続されたファイアウォール手段と、このファイアウォール手段を介して外部ネットワークに接続されファイアウォール手段の設定の変更内容を取り込む設定インターフェイス手段と、この設定インターフェイス手段を介して予め登録されている利用を許可された利用者であるかの認証をし、認証された利用者毎に設定可能な設定項目を制限し、変更内容の正当性を評価した上でファイアウォール手段の設定を変更する設定変更手段とを設ける。

【選択図】

図1



## 【特許請求の範囲】

## 【請求項 1】

内部ネットワークへの不正なアクセスを制限するファイアウォール装置において、  
前記内部ネットワークに対する不正なアクセスを制限する外部ネットワークに接続された  
ファイアウォール手段と、  
このファイアウォール手段を介して前記外部ネットワークに接続され前記ファイアウォール  
手段の設定の変更内容を取り込む設定インターフェイス手段と、  
この設定インターフェイス手段を介して予め登録されている利用を許可された利用者である  
かの認証をし、認証された利用者毎に設定可能な設定項目を制限し、変更内容の正当性  
を評価した上で前記ファイアウォール手段の設定を変更する設定変更手段と  
を備えたことを特徴とするファイアウォール装置。

10

## 【請求項 2】

前記設定インターフェイス手段が、  
WWWサーバであることを特徴とする  
請求項 1 記載のファイアウォール装置。

## 【請求項 3】

前記設定インターフェイス手段が、  
t e l n e tサーバであることを特徴とする  
請求項 1 記載のファイアウォール装置。

## 【請求項 4】

前記設定変更手段が、  
利用者端末からアクセスがあった場合に利用者の認証処理を行い、  
予め登録されている利用者であると判断した場合には予め登録されている認証された利用  
者の利用者情報に基づき設定可能な設定項目を制限し、  
前記ファイアウォール手段の当該設定項目の設定状況を調査し、  
設定可能な設定項目の設定状況を前記利用者端末に送信し、  
前記利用者端末から受信した変更内容の正当性が認められれば前記ファイアウォール手段  
に対して受信した変更内容を反映させることを特徴とする  
請求項 1 記載のファイアウォール装置。

20

## 【請求項 5】

前記設定変更手段が、  
設定変更の有効期限が満了した場合に前記ファイアウォール手段の設定を復元することを  
特徴とする  
請求項 1 若しくは請求項 4 記載のファイアウォール装置。

30

## 【請求項 6】

前記設定変更手段が、  
予めデフォルトで設定されている有効期限を用いて前記ファイアウォール手段の設定を復  
元することを特徴とする  
請求項 1 若しくは請求項 4 記載のファイアウォール装置。

## 【請求項 7】

前記設定変更手段が、  
変更内容に付加された設定変更の有効期限を用いて前記ファイアウォール手段の設定を復  
元することを特徴とする  
請求項 1 若しくは請求項 4 記載のファイアウォール装置。

40

## 【請求項 8】

前記設定変更手段が、  
変更内容に付加された設定変更の有効期限が存在する場合には、付加された有効期限を用  
い、付加されていない場合には予めデフォルトで設定されている有効期限を用いて前記フ  
ァイアウォール手段の設定を復元することを特徴とする  
請求項 1 若しくは請求項 4 記載のファイアウォール装置。

50

## 【請求項 9】

前記設定変更手段が、  
設定変更、若しくは、設定復元の内容を履歴として記憶手段に格納することを特徴とする  
請求項 1, 4, 5, 6, 7 若しくは請求項 8 のいずれかに記載のファイアウォール装置。

## 【請求項 10】

前記ファイアウォール手段が、  
前記設置変更手段からの設定状況の照会があった場合には前記設定変更手段に対して設定  
状況を送信し、  
前記設定変更手段から設定変更の要求があった場合には設定を変更し、  
前記設定変更手段から設定復元の要求があった場合には設定を復元することを特徴とする  
請求項 1 記載のファイアウォール装置。 10

## 【発明の詳細な説明】

## 【0001】

## 【発明の属する技術分野】

本発明は、内部ネットワークへの不正なアクセスを制限するファイアウォール装置に関し、特に誤設定やセキュリティの低下を招くことなくアクセス制限の一時的な変更が可能なファイアウォール装置に関する。

## 【0002】

## 【従来の技術】

従来のファイアウォール装置は内部ネットワークとインターネット等の外部ネットワークとの間に設けられて、当該ファイアウォール装置を通過するデータを全て監視して内部ネットワークに対する不正なアクセスを制限するものである。 20

## 【0003】

図 6 はこのような従来のファイアウォール装置の一例を用いたネットワークシステムを示す構成ブロック図である。図 6 において 1 は利用者端末、2 はファイアウォール装置、3 は管理者端末、100 はインターネット等の外部ネットワーク、101 はイントラネット等の内部ネットワークである。

## 【0004】

利用者端末 1 は外部ネットワーク 100 を介してファイアウォール装置 2 に接続され、ファイアウォール装置 2 は内部ネットワーク 101 に接続される。また、管理者端末 3 もまた内部ネットワーク 101 に接続される。 30

## 【0005】

また、図 7 はファイアウォール装置 2 の具体例を示す構成ブロック図である。図 7 において 2, 100 及び 101 は図 6 と同一符号を付してあり、4 は内部ネットワークに対する不正なアクセスを制限するファイアウォール手段、5 はファイアウォール手段 4 の設定の変更内容を取り込むと共に設定変更を行うための WWW (World Wide Web) サーバや t e l n e t (遠隔地から遠隔操作を行う等の仮想端末プロトコル：以下、単に t e l n e t と呼ぶ。)サーバ等の設定インターフェイス手段である。

## 【0006】

ファイアウォール手段 4 は外部ネットワーク 100 に接続され、ファイアウォール手段 4 は内部ネットワーク 101 に接続されると共に設定インターフェイス手段 5 に接続される。 40

## 【0007】

ここで、図 6 示す従来のファイアウォール装置を用いたネットワークシステムの動作を図 8 を用いて説明する。図 8 はネットワークシステムにおけるファイアウォール装置の一時的な設定変更の手順を説明するフロー図である。

## 【0008】

図 8 中 "S001" において利用者は予めファイアウォール装置 4 の管理者から管理者権限を取得して、利用者端末 1 から当該管理者権限を用いてファイアウォール装置 4 の設定インターフェイス手段 5 にアクセスする。

## 【0009】

例えば、ファイアウォール装置4の管理者権限としては、管理者用のユーザID及びパスワードそれ自体であったり、若しくは、利用者のユーザIDに対して管理者の権限を付与してもらうことである。

## 【0010】

また、例えば、設定インターフェイス手段5がWWWサーバであれば利用者端末1にインストールされた汎用のWebブラウザでアクセスし、設定インターフェイス手段5がtelnetサーバであれば利用者端末1にインストールされたtelnetクライアントソフト等を用いてアクセスする。

## 【0011】

図8中“S002”において利用者は設定インターフェイス手段5の機能を用いて利用者端末1から内部ネットワーク101にアクセスが可能になるようにファイアウォール手段4の設定を変更する。

## 【0012】

例えば、利用者がWebブラウザやtelnetクライアントソフトによって利用者端末1の画面上に表示された設定画面等を操作して設定変更を行い、利用者端末1から内部ネットワーク101へのアクセスを可能にする。

## 【0013】

そして、図8中“S003”において利用者は利用者端末1からファイアウォール手段4を通過して内部ネットワーク101にアクセスする。

## 【0014】

図8中“S004”において利用者が内部ネットワーク101への必要なアクセスが完了したと判断した場合には、図8中“S005”において利用者は設定インターフェイス手段5の機能を用いてファイアウォール手段4の設定を復元する。

## 【0015】

例えば、利用者がWebブラウザやtelnetクライアントソフトによって利用者端末1の画面上に表示された設定画面等を操作して設定の復元を行い、利用者端末1から内部ネットワーク101へのアクセスを制限させる。

## 【0016】

この結果、管理者権限により設定インターフェイス手段5にアクセスしてファイアウォール手段4の設定を変更することにより、アクセス制限の一時的な変更が可能になる。

## 【0017】

## 【発明が解決しようとする課題】

しかし、図6及び図7に示す従来例では利用者に管理者権限を与えるため、設定可能な範囲はファイアウォール手段4に関連する項目のみに限定することができず、言い換えれば、設定インターフェイス5等のファイアウォール装置2の他の機能の設定変更も可能になってしまい、誤設定による動作不良やセキュリティの低下を招いてしまうと言った問題点があった。

## 【0018】

また、ファイアウォール手段4の設定変更をする利用者が複数人いる場合に、どの設定変更がどの利用者によるものであるのかを識別することができず、セキュリティ上好ましくないと言った問題点があった。

## 【0019】

また、従来例では利用者毎に設定可能な項目を制限することができないので利用者に関係のない項目まで設定変更される恐れがあり、セキュリティの低下を招いてしまうと言った問題点があった。

## 【0020】

また、従来例では設定変更の内容の正当性を判断していないので誤設定による動作不良やセキュリティの低下を招いてしまうと言った問題点があった。

## 【0021】

10

20

30

40

50

さらに、ファイアウォール手段4のアクセス制限の一時的な解除(変更)は利用者が設定の復元を行うまで解消されないので、万が一、利用者が設定の復元を忘れた場合にはセキュリティホールとなる恐れがあり、セキュリティの低下を招いてしまうといった問題点があった。

従って本発明が解決しようとする課題は、誤設定やセキュリティの低下を招くことなくアクセス制限の一時的な変更が可能なファイアウォール装置を実現することにある。

#### 【0022】

##### 【課題を解決するための手段】

このような課題を達成するために、本発明のうち請求項1記載の発明は、  
内部ネットワークへの不正なアクセスを制限するファイアウォール装置において、  
前記内部ネットワークに対する不正なアクセスを制限する外部ネットワークに接続された  
ファイアウォール手段と、このファイアウォール手段を介して前記外部ネットワークに接  
続され前記ファイアウォール手段の設定の変更内容を取り込む設定インターフェイス手段  
と、この設定インターフェイス手段を介して予め登録されている利用を許可された利用者  
であるかの認証をし、認証された利用者毎に設定可能な設定項目を制限し、変更内容の正  
当性を評価した上で前記ファイアウォール手段の設定を変更する設定変更手段とを備えた  
ことにより、誤設定やセキュリティの低下を招くことなくアクセス制限の一時的な変更が  
可能になる。

10

#### 【0023】

請求項2記載の発明は、  
請求項1記載の発明であるファイアウォール装置において、  
前記設定インターフェイス手段が、  
WWWサーバであることにより、誤設定やセキュリティの低下を招くことなくアクセス制  
限の一時的な変更が可能になる。

20

#### 【0024】

請求項3記載の発明は、  
請求項1記載の発明であるファイアウォール装置において、  
前記設定インターフェイス手段が、  
telnetサーバであることにより、誤設定やセキュリティの低下を招くことなくアク  
セス制限の一時的な変更が可能になる。

30

#### 【0025】

請求項4記載の発明は、  
請求項1記載の発明であるファイアウォール装置において、  
前記設定変更手段が、  
利用者端末からアクセスがあった場合に利用者の認証処理を行い、予め登録されている利  
用者であると判断した場合には予め登録されている認証された利用者の利用者情報に基づ  
き設定可能な設定項目を制限し、前記ファイアウォール手段の当該設定項目の設定状況を  
調査し、設定可能な設定項目の設定状況を前記利用者端末に送信し、前記利用者端末から  
受信した変更内容の正当性が認められれば前記ファイアウォール手段に対して受信した変  
更内容を反映させることにより、誤設定やセキュリティの低下を招くことなくアクセス制  
限の一時的な変更が可能になる。

40

#### 【0026】

請求項5記載の発明は、  
請求項1若しくは請求項4記載の発明であるファイアウォール装置において、  
前記設定変更手段が、  
設定変更の有効期限が満了した場合に前記ファイアウォール手段の設定を復元すること  
により、利用者が設定の復元を忘れた場合であってもセキュリティホールとはならず、セキ  
ュリティの低下を防止することができる。

#### 【0027】

請求項6記載の発明は、

50

請求項 1 若しくは請求項 4 記載の発明であるファイアウォール装置において、  
前記設定変更手段が、

予めデフォルトで設定されている有効期限を用いて前記ファイアウォール手段の設定を復元することにより、利用者が設定の復元を忘れた場合であってもセキュリティホールとはならず、セキュリティの低下を防止することができる。

【0028】

請求項 7 記載の発明は、

請求項 1 若しくは請求項 4 記載の発明であるファイアウォール装置において、  
前記設定変更手段が、

変更内容に付加された設定変更の有効期限を用いて前記ファイアウォール手段の設定を復元することにより、利用者が設定の復元を忘れた場合であってもセキュリティホールとはならず、セキュリティの低下を防止することができる。 10

【0029】

請求項 8 記載の発明は、

請求項 1 若しくは請求項 4 記載の発明であるファイアウォール装置において、  
前記設定変更手段が、

変更内容に付加された設定変更の有効期限が存在する場合には、付加された有効期限を用い、付加されていない場合には予めデフォルトで設定されている有効期限を用いて前記ファイアウォール手段の設定を復元することにより、利用者が設定の復元を忘れた場合であってもセキュリティホールとはならず、セキュリティの低下を防止することができる。 20

【0030】

請求項 9 記載の発明は、

請求項 1, 4, 5, 6, 7 若しくは請求項 8 のいずれかに記載の発明であるファイアウォール装置において、

前記設定変更手段が、

設定変更、若しくは、設定復元の内容を履歴として記憶手段に格納することにより、設定変更等がどの利用者によるものであるのかを特定することが可能になる。

【0031】

請求項 10 記載の発明は、

請求項 1 記載の発明であるファイアウォール装置において、 30

前記ファイアウォール手段が、

前記設置変更手段からの設定状況の照会があった場合には前記設定変更手段に対して設定状況を送信し、前記設定変更手段から設定変更の要求があった場合には設定を変更し、前記設定変更手段から設定復元の要求があった場合には設定を復元することにより、誤設定やセキュリティの低下を招くことなくアクセス制限の一時的な変更が可能になる。

【0032】

【発明の実施の形態】

以下本発明を図面を用いて詳細に説明する。図 1 は本発明に係るファイアウォール装置の  
一実施例を用いたネットワークシステムを示す構成ブロック図である。

【0033】

図 1 において 6 は利用者端末、7 はファイアウォール装置、8 は管理者端末、100a はインターネット等の外部ネットワーク、101a はイントラネット等の内部ネットワークである。 40

【0034】

利用者端末 6 は外部ネットワーク 100a を介してファイアウォール装置 7 に接続され、ファイアウォール装置 7 は内部ネットワーク 101a に接続される。また、管理者端末 8 もまた内部ネットワーク 101a に接続される。

【0035】

また、図 2 はファイアウォール装置 7 の具体例を示す構成ブロック図である。図 2 において 7, 100a 及び 101a は図 1 と同一符号を付してあり、9 は内部ネットワークに対 50

する不正なアクセスを制限するファイアウォール手段、10はファイアウォール手段9の設定の変更内容を取り込むためのWWWサーバやtelnetサーバ等の設定インターフェイス手段、11はユーザ認証や正当性の判断等を行いファイアウォール手段9の設定変更を行う設定変更手段、12は変更履歴等が格納される記憶手段である。

【0036】

ファイアウォール手段9は外部ネットワーク100aに接続され、ファイアウォール手段9は内部ネットワーク101aに接続されると共に及び設定インターフェイス手段10に接続される。

【0037】

また、設定変更手段11の2つの入出力の内、一方の入出力が設定インターフェイス手段10に接続され、他方の入出力がファイアウォール手段9に接続される。さらに、設定変更手段11の出力が記憶手段12に接続される。

【0038】

ここで、図1示す実施例であるファイアウォール装置7を用いたネットワークシステムの動作を図3、図4及び図5を用いて説明する。図3はネットワークシステムにおける利用者端末6の動作を説明するフロー図、図4は設定変更手段11の動作を説明するフロー図、図5はファイアウォール手段9の動作を説明するフロー図である。

【0039】

設定変更手段11には予め管理者により利用を許可する利用者の認証情報及び利用者情報が登録されている。

【0040】

例えば、認証情報としては利用者毎に設定されたユーザID及びパスワード等であり、利用者情報としては当該利用者がファイアウォール手段9に対して変更可能な項目等である。

【0041】

図3中”S101”において利用者端末6は設定インターフェイス手段10を介して設定変更手段11に接続する。そして、図3中”S102”において利用端末6は利用者が入力した認証情報を設定インターフェイス手段10を介して設定変更手段11に送信する。

【0042】

図3中”S103”において利用者端末6は設定インターフェイス手段10を介して設定変更手段11からファイアウォール手段9の設定状況を受信したか否かを判断し、もし、設定状況を受信した場合には図3中”S104”において設定状況を利用者端末6の表示手段に表示させる。

【0043】

図3中”S105”において利用者端末6は設定インターフェイス手段10の機能を用いてファイアウォール手段9の設定の変更をする。言い換えれば、設定の変更内容を設定インターフェイス手段10を介して設定変更手段11に送信する。この時、利用者端末6は同時に当該設定変更の有効期限を変更内容に付加して送信する。

【0044】

例えば、利用者はWebブラウザやtelnetクライアントソフトによって利用者端末6の画面上に表示された設定画面等を実行して設定の変更を行い、利用者端末6から内部ネットワーク101aへのアクセスを可能にする変更内容を設定インターフェイス手段10を介して設定変更手段11に送信する。

【0045】

図3中”S106”において利用者端末6は設定インターフェイス手段10を介して設定変更手段11から設定変更が完了した旨の通知を受信したか否かを判断し、もし、設定変更の完了通知を受信した場合には図3中”S107”においてファイアウォール手段9を介して内部ネットワーク101aにアクセスする。

【0046】

10

20

30

40

50



一方、図4中“S201”において設定変更手段11は設定インターフェイス手段10を介して利用者端末6からのアクセスがあったか否かを判断する。もし、利用者端末6からのアクセスがあった場合には図4中“S202”において利用者の認証処理を行う。

【0047】

例えば、設定変更手段11はアクセスのあった利用者端末6のIP（Internet Protocol）アドレス等の必要な情報を取得すると共に利用者端末6から送信されてきた認証情報を受信し、予め登録されている利用を許可する利用者であるか否かを確認する。

【0048】

そして、図4中“S203”において設定変更手段11は受信した認証情報から予め登録されている利用者でないと判断した場合には、図4中“S201”のステップに戻る。 10

【0049】

もし、図4中“S203”において設定変更手段11は受信した認証情報から予め登録されている利用者であると判断した場合には、図4中“S204”において予め登録されている認証された利用者の利用者情報と、取得したIPアドレスとに基づき認証された利用者が設定可能な設定項目を決定し、言い換えれば、設定項目を制限し、ファイアウォール手段9の当該設定項目の設定状況を調査する。

【0050】

図4中“S205”において設定変更手段11は設定インターフェイス手段10を介して認証された利用者が設定可能な設定項目と、調査結果である設定可能な設定項目の設定状況を利用者端末6に送信する。 20

【0051】

そして、図4中“S206”において設定変更手段11は利用者端末6からの設定の変更内容を受信するまで待機する。

【0052】

図4中“S207”において設定変更手段11は受信した変更内容の正当性を評価し、変更内容に矛盾や問題点等がなければ、言い換えれば、正当性が認められればファイアウォール手段9に対して受信した変更内容を反映させる。

【0053】

例えば、受信した変更内容が“利用者端末6から内部ネットワーク101aへのアクセスを可能にする”内容であった場合、設定変更手段11はファイアウォール手段9に対して利用者端末6から内部ネットワーク101aへのアクセスを許可させる。 30

【0054】

もし、図4中“S207”において設定変更手段11は受信した変更内容の正当性を評価し、変更内容に矛盾や問題点等があれば、設定変更手段11は設定インターフェイス手段10を介して利用者端末6に警告を与える。

【0055】

例えば、設定変更手段11は取得した利用者端末6のIPアドレスが“10.0.xx.105”であるのに、変更内容に記載された内部ネットワーク101へのアクセスを許可させるIPアドレスが“10.0.xx.15”である場合には誤入力の可能性が高いのでその旨利用者端末6に警告を与える。 40

【0056】

図4中“S208”において設定変更手段11は設定変更の内容を履歴として記憶手段12に格納する。例えば、日時、認証された利用者のユーザID、変更内容等を履歴として記憶手段12に記録しておく。

【0057】

図4中“S209”において設定変更手段11は設定インターフェイス手段10を介して設定変更が完了した旨の通知を利用者端末6に対して送信する。

【0058】

図4中“S210”において設定変更手段11は設定変更完了から時間が、受信した変更 50

内容に付加されていた有効期限を超過するまで待機し、言い換えれば、設定変更の有効期限が満了するまで待機する。

【0059】

設定変更の有効期限が満了した場合、図4中“S211”において設定変更手段11はファイアウォール手段9に対して設定を元の状態に復元し、図4中“S212”において設定の復元の内容を履歴として記憶手段12に格納する。例えば、日時、認証された利用者のユーザID、復元内容等を履歴として記憶手段12に記録しておく。

【0060】

また、図5中“S301”においてファイアウォール手段9は設定変更手段11からの設定状況の照会があったか否かを判断し、もし、設定状況の照会があった場合には図5中“S302”において設定変更手段11に対して設定状況を送信して図5中“S301”に示すステップに戻る。 10

【0061】

もし、図5中“S301”において設定状況の照会が無かった場合には、図5中“S303”においてファイアウォール手段9は設定変更手段11から設定変更の要求があったか否かを判断し、もし、設定変更の要求があった場合には設定を変更して図5中“S301”に示すステップに戻る。

【0062】

もし、図5中“S303”において設定変更の要求が無かった場合には、図5中“S305”においてファイアウォール手段9は設定変更手段11から設定復元の要求があったか否かを判断し、もし、設定復元の要求があった場合には設定を復元して図5中“S301”に示すステップに戻る。 20

【0063】

もし、図5中“S305”において設定復元の要求が無かった場合には、図5中“S301”に示すステップに戻る。

【0064】

この結果、設定変更手段11がユーザ認証を行い、認証された利用者毎に設定可能な設定項目を制限し、変更内容の正当性を評価した上でファイアウォール手段9の設定を変更することにより、誤設定やセキュリティの低下を招くことなくアクセス制限の一時的な変更が可能になる。 30

【0065】

また、設定変更手段11がファイアウォール手段9の設定変更及び設定復元の内容を履歴として記憶手段12に格納することにより、設定変更等がどの利用者によるものであるのかを特定することが可能になる。

【0066】

さらに、設定変更手段11が設定変更の有効期限が満了した場合に設定を復元することにより、万が一、利用者が設定の復元を忘れた場合であってもセキュリティホールとはならず、セキュリティの低下を防止することができる。

【0067】

なお、図1に示す実施例を用いたネットワークシステムでは外部ネットワーク100aに接続された利用者端末6からのファイアウォール手段9の設置変更について説明しているが、勿論、内部ネットワーク101aに接続された利用者端末からであっても同様にファイアウォール手段9の設定変更が可能である。 40

【0068】

また、図3の説明に際しては利用者端末6が設定変更の有効期限を変更内容に付加して送信する旨例示されているが、設定変更手段11が予めデフォルトで設定されている有効期限を使用しても良い。

【0069】

さらに、設定変更手段11が利用者端末6から変更内容に付加された設定変更の有効期限が存在する場合には、付加された有効期限を用い、付加されていない場合には予めデフォ 50

ルトで設定されている有効期限を用いても良い。

【0070】

これらの場合には、利用者端末6が設定変更の有効期限を変更内容に付加して送信する必要性がなくなるので、有効期限の付加し忘れによるセキュリティの低下を防止することができる。

【0071】

また、図2に示す設定変更手段11の機能をネットワークルータに具備させることにより、ネットワークルータに適用することが可能になる。

【0072】

また、図2に示す設定変更手段11の機能をファイアウォール・ソフトウェアに具備させることにより、ファイアウォール・ソフトウェアに適用することが可能になる。 10

【0073】

また、図2に示す設定変更手段11の機能をネットワークルータ管理ソフトウェアに具備させることにより、ネットワークルータ管理ソフトウェアに適用することが可能になる。

【0074】

また、図4に示す設定変更手段の動作説明では認証された利用者の利用者情報と取得したIPアドレスに基づき認証された利用者が設定可能な設定項目を制限している旨例示されているが、認証された利用者の利用者情報のみに基づき認証された利用者が設定可能な設定項目を制限しても構わない。

【0075】

20

【発明の効果】

以上説明したことから明らかなように、本発明によれば次のような効果がある。

請求項1, 2, 3, 4及び請求項10の発明によれば、設定変更手段がユーザ認証を行い、認証された利用者毎に設定可能な設定項目を制限し、変更内容の正当性を評価した上でファイアウォール手段の設定を変更することにより、誤設定やセキュリティの低下を招くことなくアクセス制限の一時的な変更が可能になる。

【0076】

また、請求項5, 6, 7及び請求項8の発明によれば、設定変更手段が設定変更の有効期限が満了した場合に設定を復元することにより、万が一、利用者が設定の復元を忘れた場合であってもセキュリティホールとはならず、セキュリティの低下を防止することができる。 30

【0077】

また、請求項9の発明によれば、設定変更手段がファイアウォール手段の設定変更及び設定復元の内容を履歴として記憶手段に格納することにより、設定変更等がどの利用者によるものであるのかを特定することが可能になる。

【図面の簡単な説明】

【図1】本発明に係るファイアウォール装置の一実施例を用いたネットワークシステムを示す構成ブロック図である。

【図2】ファイアウォール装置の具体例を示す構成ブロック図である。

【図3】ネットワークシステムにおける利用者端末の動作を説明するフロー図である。 40

【図4】設定変更手段の動作を説明するフロー図である。

【図5】ファイアウォール手段の動作を説明するフロー図である。

【図6】従来のファイアウォール装置の一例を用いたネットワークシステムを示す構成ブロック図である。

【図7】ファイアウォール装置の具体例を示す構成ブロック図である。

【図8】ネットワークシステムにおけるファイアウォール装置の一時的な設定変更の手順を説明するフロー図である。

【符号の説明】

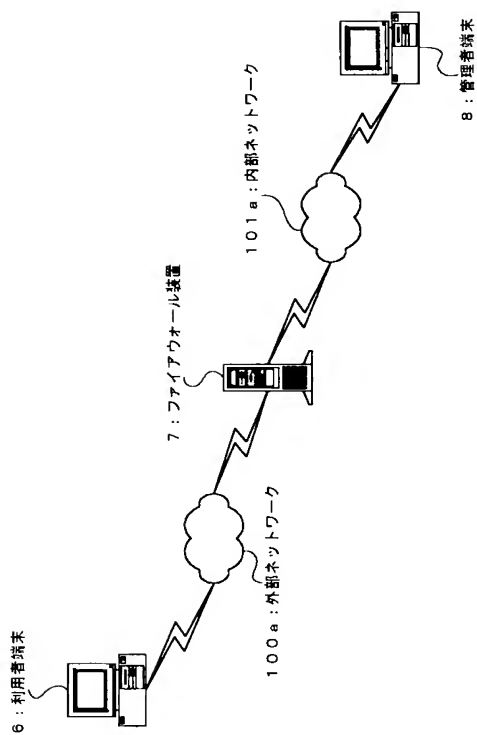
1, 6 利用者端末

2, 7 ファイアウォール装置

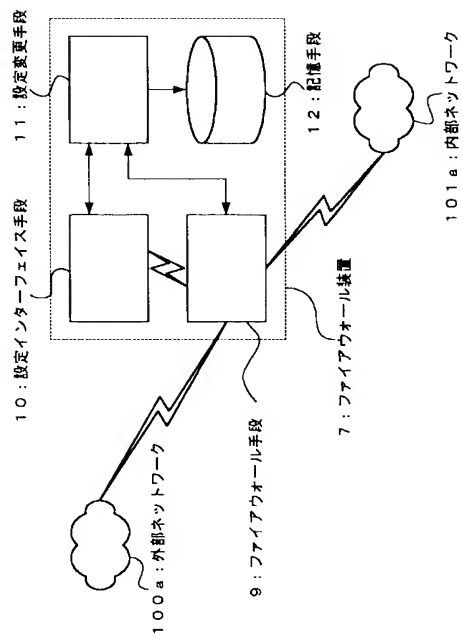
50

- 3, 8 管理者端末
- 4, 9 ファイアウォール手段
- 5, 10 設定インターフェイス手段
- 11 設定変更手段
- 12 記憶手段
- 100, 100a 外部ネットワーク
- 101, 101a 内部ネットワーク

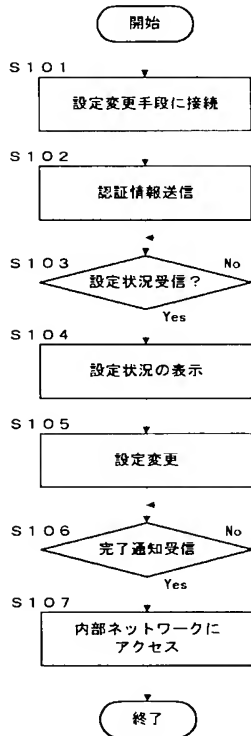
【図 1】



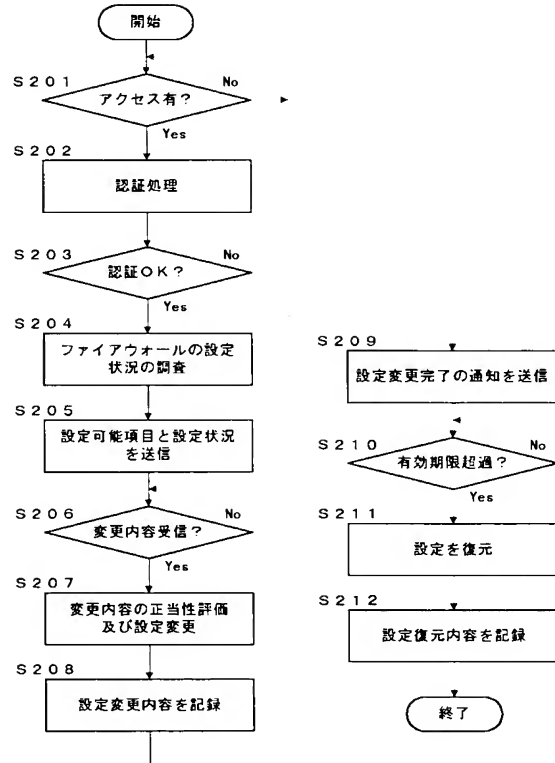
【図 2】



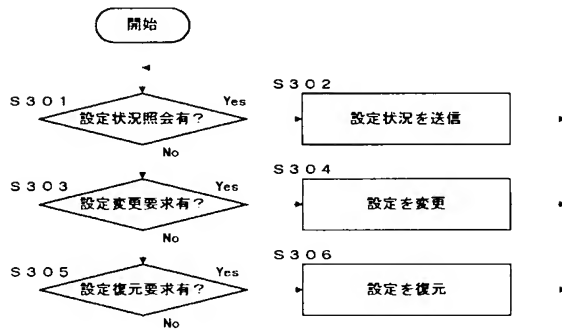
【図 3】



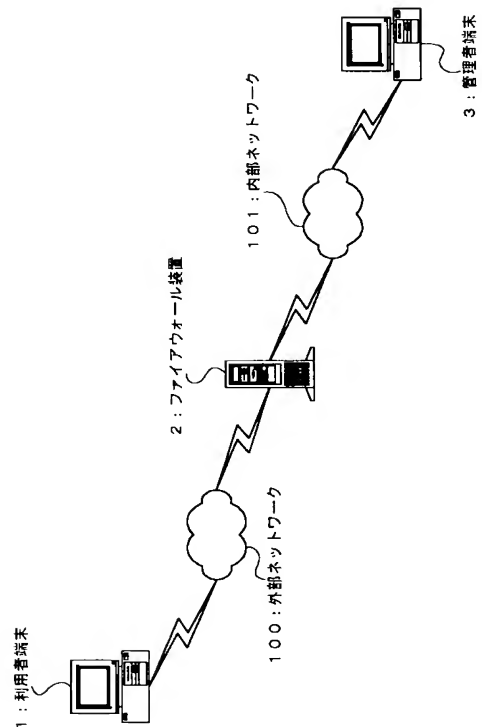
【図 4】



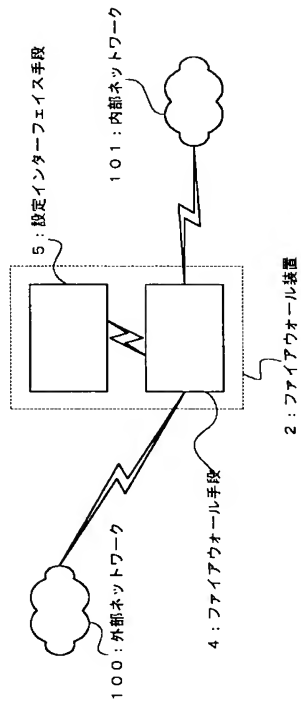
【図 5】



【図 6】



【図 7】



【図 8】

